IN THE SPECIFICATION

Please replace the paragraph beginning at page 1, line 8 with the following amended paragraph:

Recently there ~~have~~ has been much development in the area of portable data storage devices having non-volatile solid state memory units, such as flash memories. A seminal patent application in this area, PCT/SG00/00029, "Portable Data Storage Device", describes a memory device which can be directly plugged into the socket of a computer using an integral male USB plug. The size of the device is such that it is capable, for example, of being fully enclosed within a closed fist, and is in this sense portable. It is able to receive data from one computer system, and transfer it to another computer system, just like a magnetic disk or CD-RW disk.

Please replace the paragraph beginning at page 2, line 6 with the following amended paragraph:

PCT/SG01/00136 describes a portable data storage device which is arranged for wireless communication with a host, e.g. by radio, for receiving data and subsequently regenerating it. The device is thus capable of transferring data between computer systems which are capable of this wireless data transmission. PCT/SG03/00152 describes an enhancement of this system in which the data storage device includes a pointer, so that ~~it can~~ a user can move it to act as a convenient data input device.

Please replace the paragraph beginning at page 5, line 7 with the following amended paragraph:

Furthermore, the device preferably ~~include~~ includes a compression algorithm for exploiting any redundancy in data received by the device to compress it before storing it in the non-volatile memory, and a decompression engine to regenerate the data before it is transmitted from the device.

Please replace the paragraph beginning at page 6, line 27 with the following amended paragraph:

Alternatively, the section 7 may be provided as a section for wireless data transmission/reception to the host (e.g. without physical contact of the memory device and the host). ~~It~~ In this case, ~~it may~~ the plug 9 is replaced by an antenna, and the interface device 11 is replaced by a device for using the antenna for wireless transmission/reception of data. For example, these two units may function together to provide an interface according to a wireless standard, such as WLAN or Bluetooth.

Please replace the paragraph beginning at page 9, line 6 with the following amended paragraph:

Note that these modes of operation are described, for the sake of simplicity, without reference to the concept mentioned above of verifying user identity using the biometric sensor [[7]] 5. However, it is to be understood that any of the processes described above may optionally include steps (e.g. after data is requested from the device) in which biometric data is input to the biometric sensor [[7]] 5, and the

identity of that data with biometric data pre-stored in the device is checked, before the device performs any further steps of the process.

Please replace the paragraph beginning at page 9, line 28 with the following amended paragraph:

The MCU 1 then encrypts the private key K using the secret key i and transmits the encrypted private key K to the host (step 3). The device further transmits the data requested by the host (step 4a). Note that this requested data may optionally be encoded by the MCU before it is transmitted to the host, e.g. using the public key Z. This can be done in various ways, such as by a symmetric encryption (e.g. using i), or using the private key K. One preferred possibility is to generate second set of public/private keys, transmit the second private key to the host encoded (e.g. using i ) such that the host can decode it, and then transmitting the data encoded using the second public key such that the host can decrypt it using the second private key.

Please replace the paragraph beginning at page 10, line 12 with the following amended paragraph:

In step 5a, the host decodes the private key K using the secret key i it already knew. In the case that the requested data was encrypted using the public key Z, the host decodes it using K.

Please replace the paragraph beginning at page 12, line 6 with the following amended paragraph:

In step 3, the device (normally the MCU 1) generates a digital signature using the requested data A. It may do this by the sub-steps of hashing the requested data A to form a hash result A' (step 3.1), and then encrypting it with the private key K (step 3.2). The host then transmits the data, the digital signature and the public key Z to the host (step 4b).

Please replace the paragraph beginning at page 12, line 6 with the following amended paragraph:

The host uses the pubic key and the requested data A to verify that the requested data A matches the digital signature (step 5b). For example, it can do this by using the requested data A to generate a hash result B', and decrypting the digital signature using the public key Z to form a result C'. If B' is equal to C', then this indicates that the data is correctly received. A hacker will not be able to fool the host unless he can modify A while keeping still keeping it such that it is still consistent with the digital signature (and still meeting any other predetermined characteristics--e.g. if A is a file which is intended to operate with an application, the host will be able to detect the modification if the file it receives is not compatible with that application), which in general is an extremely difficult computational task. Most modifications of A which keep its hash value will change its characteristics in other ways, e.g. make it meaningless in the context for which it is intended.

Please replace the paragraph beginning at page 14, line 1 with the following amended paragraph:

Another possible refinement of the second mode of operation of the device is that the data A may be supplemented with data which is not necessarily taken from the memory 3. In particular, it may be supplemented with biometric data received by the biometric sensor [[7]] 5. Thus, this data too may be securely transmitted to the host (in the sense that the host can verify that is has received exactly the biometric data transmitted by the device), and the host can verify that it matches biodata to which the host has access.